雲端服務模式數位證據之識別、蒐集、擷取、保全及驗證程序

陳受湛[1] 鄧思源[2] 萬幼筠[3] 陳威棋[4]
法務部調查局資通安全處 勤業眾信聯合會計師事務所
dan-chen@seed.net.tw[1] buyer92@mjib.gov.tw[2] thomaswan@deloitte.com.tw[3]
ikewchen@deloitte.com.tw[4]

摘要

雲端服務之數位鑑識作業因雲端資料儲存特性及雲端業者與使用者各自管理權限問題，與一般數位鑑識有顯著差異，鑑識人員若仍依循舊有程序將無法完整識別、蒐集必要之雲端數位證據。本研究彙整國內外相關文獻與法令規範，並透過建置模擬環境實際執行各種雲端服務後取得數位證據留存種類，進而提出最適於執行各種雲端鑑識之建議流程。

關鍵詞：雲端鑑識、雲端數位證據、數位鑑識程序

Identification, Collection, Acquisition, Preservation and Authentication of the Digital Forensic in Cloud environment

CHEN, SOU-CHAN[1], TENG, SZU-YAUN[2], Wan, You-Yen[3], CHEN, WEI CHI[4]
Ministry of Justice Investigation Bureau Information Security Department, Deloitte Taiwan
Dan-chen@seed.net.tw[1], buyer92@mjib.gov.tw[2], thomaswan@deloitte.com.tw[3],
ikewchen@deloitte.com.tw[4]

Abstract

The method of the data storage and user control in cloud environment are significantly different than traditional digital forensic methods. Digital evidence in the cloud environment will be unable to fully identify and collected if digital forensic personal follows the traditional process. This article contains related researches and regulations from different nation. Furthermore, collects the digital evidence with the implementation of the cloud service through virtual environment, and provide the digital forensic process suitable for all types of cloud services.

Keywords: Cloud Forensics, Cloud Digital Forensic, Digital Forensic process

壹、前言

雲端服務近年已成為民眾大量使用之新興科技之一，且隨著各種新技術突破促使資料傳輸、分享或取得更為方便快速。在前述技術運用於日常生活與商業環境所帶來的極大便利性的同時，網路犯罪者們亦會隨著網路、資訊科技及雲端運算的進步發展，不斷改善他們的攻擊技巧與工具。

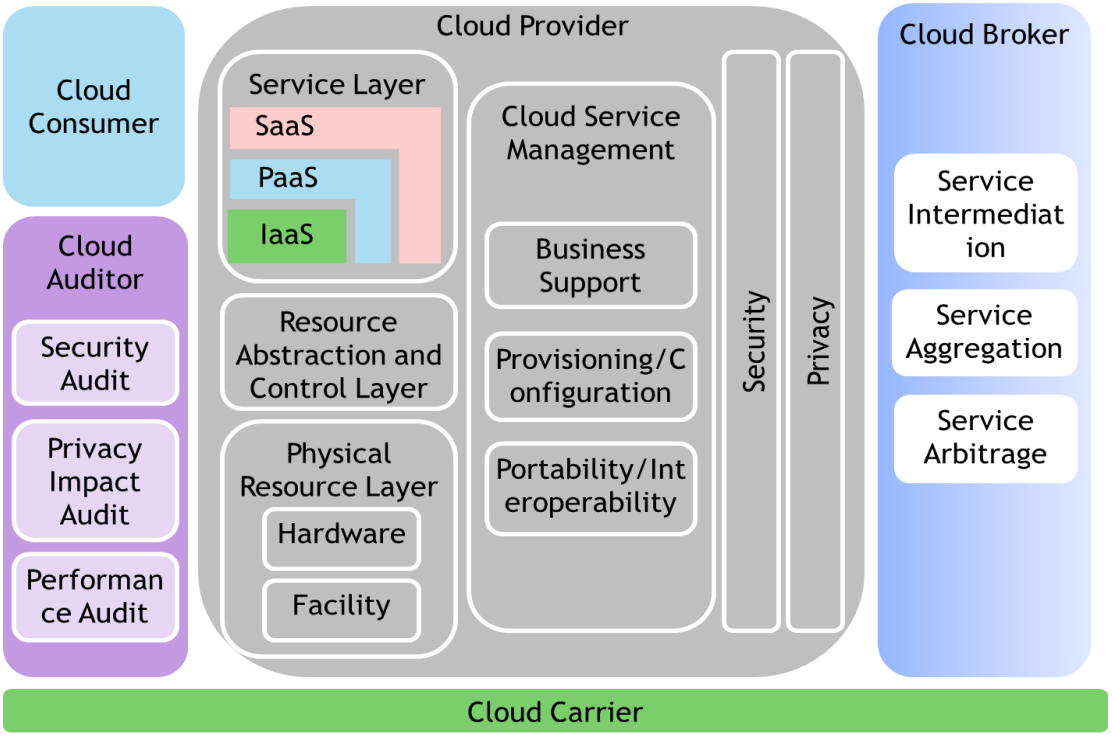
有別於一般資訊設備，雲端服務可透過大量分散式運算、資料儲存及虛擬化技術，提供使用者更為便利且不易中斷之網路服務，但同時也讓傳統數位鑑識無法適用於雲端鑑識中，因為識別要點不再是單純辨識潛在數位證據，而是需要從識別使用者曾執行過哪些雲端服務開始。且蒐集標的不再僅是實體可被封存之電腦硬碟，而可能是雲端服務業者機房中大型磁碟陣列中的其中一些磁軌。

為協助鑑識人員解決執行雲端數位鑑識作業可能遇到之困境，本研究中透過研究國內外雲端鑑識相關文獻、建置雲端服務模擬環境及實際測試後取得各種雲端服務可能存在之數位證據種類，提出符合國際最佳實務之雲端證據處理及鑑識作業程序建議。鑑識人員於雲端鑑識作業識別階段可藉由本研究之成果提高識別能力，瞭解判別有無雲端服務之數位證據種類、所在路徑及判別方式。另一方面，鑑識人員亦可於雲端鑑識作業蒐集階段參照本研究之成果，完整蒐集所有雲端數位證據，提高蒐集作業完整性。

貳、 文獻探討

一、雲端服務模式

雲端服務主要透過網際網路連線，提供使用者從遠端使用服務，根據 NIST SP800-145[14]中針對雲端服務種類之定義，共分為 IaaS、PaaS 及 SaaS 三種模式，NIST 另於 SP500-292[5]中定義完整雲端服務架構，如下圖一所示。



圖一： NIST SP500-292 中所提出之雲端架構[5]

(一) 架構即服務(Infrastructure as a Service , IaaS)

提供使用者處理器、儲存空間、網路或其他運算資源，使用者可以依自身需求，彈性取得相關運算資源而不需重新建置軟硬體環境，並可減少維護資訊設備費用且無須顧慮設備折舊汰換等問題。如國外 Amazon EC2 及國內 hicloud VPC 皆屬於此類服務。

(二) 平台即服務(Platform as a Service , PaaS)

程式開發者可於 PaaS 服務供應商所建構之基礎架構平台直接開發應用程式，利用既有軟體套件減少程式開發成本，並可透過 SaaS 服務模式提供給其他使用者。於 PaaS 中，開發者可以設計及控制應用程式，但無法變更服務商所提供之基礎架構。本類型服務較少，以 Google GAE 與 Microsoft Azure 較為知名。

(三) 軟體即服務(Software as a Service, SaaS)

在一般 SaaS 服務運作模式中，使用者可針對需求，以租賃方式使用軟體功能。軟體服務供應商將軟體安裝於伺服器中，並確保使用者可透過網路瀏覽器執行該軟體功能。

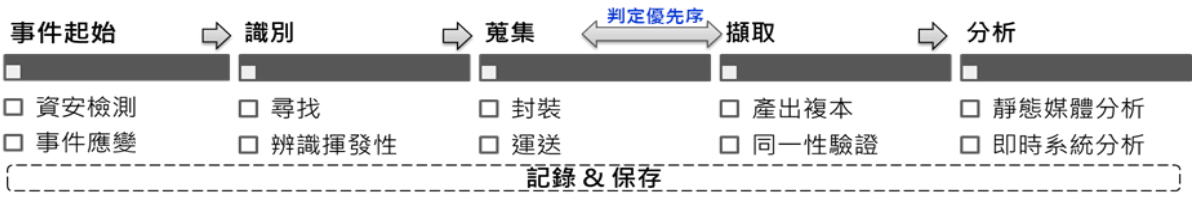
使用者可避免購置過多軟硬體設備或安裝大量軟體，即可使用最新軟體服務。本類型延伸變化服務很多，以網頁郵件(Webmail)、網頁行事曆(如 Google Calendar)與網頁共同協作平台(如 Google Drive)較常使用。

(四) 儲存空間即服務(Storage as a Service, StaaS)

StaaS 為最常見之雲端服務之一，使用者可以透過免費或付費方式，租賃服務供應商之網路儲存空間，藉以進行資料儲存、分享或備份，節省購置及維護儲存媒體之費用。此類雲端服務為 SaaS 之變化型，常見網路產品為 Dropbox、OneDrive 等網路儲存空間產品。

二、雲端作業鑑識程序

國際標準化組織(International Organization for Standardization，ISO)為一製作國際通用標準之國際組織，其成員為各國國家標準機構或主要公司之代表，總部設於瑞士日內瓦。該組織針對資訊安全事件提出 ISO27041:2015[10]及 ISO27042:2015[11]等一系列技術性的數位鑑識標準規範及技術指引，包含事件調查程序、數位證據處理、數位證據分析解讀等，從事件起始到提出證據之過程可整合為下圖所示。



圖二： ISO 體系對數位鑑識之建議程序(本研究整理)

其中，ISO27037:2012[9]規範內容係針對數位鑑識的現場處理步驟提出指引，共分為識別(Identification)、蒐集(Collection)、萃取(Acquisition)及保存(Preservation)四個階段，以下分別概述各階段之內容及要求。

(一) 識別階段(Identification)

識別階段時，鑑識人員需至犯罪現場辨識任何可能含有數位證據之任何儲存媒體、文件、紙張、電腦及網路設備等。經過完整識別可能存有數位證據之設備後，相關人員應決定是否在下一個處理程序進行蒐集或萃取。

(二) 蒐集階段(Collection)

數位證據之存在狀態有多種可能，如刪除、隱藏等。而包含數位證據之設備可能有多種不同狀態，如正在運作或關閉等，鑑識人員需根據蒐證標的設備之狀態決定使用何種方式及工具進行蒐集數位證據，另外，此階段必須在對數位證據最小程度破壞且能取得最完整資料之方式進行蒐集。

(三) 擷取階段(Acquisition)

執行本階段作業之相關人員應採用適合且不會破壞數位證據之萃取方式及工具，完整重建數位證據、記錄詳細過程及驗證產出之證據副本。

(四) 保存階段(Preservation)

保存階段應保護數位證據及相關證物不被竄改或破壞，且應開始於整個數位證據處理程序之初，並持續至處理程序結束。

針對不同雲端服務模式之鑑識作業程序之議題，雲端安全聯盟(CSA , Cloud Security Alliance)指出於實體資訊環境中，傳統的數位鑑識調查無法完全套用在雲端服務的環境中，故提出「Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing」[2]，針對數位證物識別、收集、獲得與保存等作業程序，提供資訊安全事件調查過程之依循標準與比較，整理較重要項目如下表一

表一： ISO27037 對應雲端鑑識要點

章節	**ISO/IEC 27037**:2012	對應之雲端鑑識要點
5.3.3 可重複性	當使用同樣的測量程序、方法及工具並於同樣的情況時，其結果是可重複的	雲端環境中可重複性變得很有挑戰性，以 Snapshot(快照)為例，針對雲端服務環境做兩次一樣動作之 Snapshot 作業亦無法做出一樣之複本，故其只限於 Snapshot 作業流程具備可重複性。

5.4.2 識別	進行搜尋、識別數位證據時，應根據下列原則： ● 揮發性資料優先擷取 ● 將損壞數位證據之程度降到最小 ● 識別隱藏之數位證據 ● 瞭解識別數位證據是困難的	識別特定雲端服務： ● SaaS：應用程式日誌(如認證失敗)、效能問題、儲存空間等 ● PaaS：應用程式日誌、API、程式更新狀態、系統告警、防毒軟體日誌等 ● IaaS：系統日誌、記憶體資料、快照或備份檔案、網路設備日誌
5.4.3 蒐集	蒐集是數位證據處理中的一環，包含從現場移動至鑑識實驗室或可控制之環境中，待進行後續擷取作業	由於雲端架構特性，擷取通常優先於蒐集，以避免影響數位證據。惟蒐集雲端數位證據經常只能通過 CSP 業者，而非租戶
5.4.4 擷取	擷取為一建立數位證據副本之步驟	由於雲端架構中，並無實體設備，數位證據以檔案型態存在於雲端服務中，擷取作業需針對邏輯檔案而非實體儲存媒體
7.1.1.3 蒐集標的之判斷	必須判斷並蒐集潛在證據	在雲端服務中，潛在的數位證據非常可能是碎裂及分散於不同的儲存媒體中。因此，或許無法蒐集實體證據(如硬碟)。雲端環境中，擷取通常是取得數位證據複本最適當的方式。但若為行動裝置(雲端軟體的行動客戶)則可被蒐集。
7.1.3.4 部份擷取	當系統容量太大、需緊急處理之系統、僅需取得部份資訊或法令狀約束之四種情況下，鑑識人員可執行部份擷取	在雲端環境中，擷取通常都是部分擷取，因為這樣才能符合標準要求。
7.1.3.5 儲存媒體	鑑識人員會遇到多種不同種類之儲存媒體，應記錄其位置並進行蒐集或現場擷取	在雲端環境中，資料通常會被存放於大型磁碟陣列中，其中可能存在多個複本或備份檔案，但檔案或資料可能分散於不同的實體位置存放，導致難以記錄或蒐集。

7.2.1 連網設備之識別	於網路連結之主機環境中，很難確定潛在數位證據存放位置	因鑑識人員無法實際取得雲端實體資料媒體，且雲端資料可能分散於不同位置，並可能會有不同的管轄權。建議鑑識人員瞭解標的服務之整體架構(如網路拓樸、系統架構、資料流、IP 位址及資料儲存空間等資訊)。除此之外，雲端資料容易被刪除或覆蓋，故雲端鑑識需要更快速之反應及處理能力。
	在獲得或收集任何資料之前，事件現場應透過拍照記錄,錄影或素描詳實記錄。此記錄作業應考量費用、時間、可提供的資源和優先權。	若無法直接取得雲端服務相關資料，蒐集本地端之實體或電子文件(如雲端服務使用流程或規定、雲端服務商提供之合約或條款等)變得至關重要
	審慎評估設備或媒體狀態，進行斷電或取出裝置	與一般數位鑑識不同，雲端服務之相關資料建議可透過非破壞性之取證方式(如 Snapshot)或針對虛擬化平台之特性或功能(如虛擬主機資源管理介面)進行蒐集，避免重新開機甚至關機等操作

另於周瑞國等數位學者[19]之研究指出於雲端安全之數位證據鑑識標準作業程序(CCS-DEFSOP)，可進一步提供已導入或通過 ISO/IEC 27001 之企業組織及政府機關面對未來雲端運算環境之安全服務評估參考資料或檢查項目(Checklist)。於 Yunting 等數位學者[18]與 Zawoad[16]的研究分別針對基於 ISO/IEC 27037:2012[9]之四步驟提出適用於雲端鑑識案件之基本程序，包含識別、蒐集、分析及呈現階段，如下圖三所示；其他國外學者亦針對雲端鑑識提出建議作業程序，整理如下表二。

圖三： 國外學者提出基於 ISO27037 之雲端鑑識程序

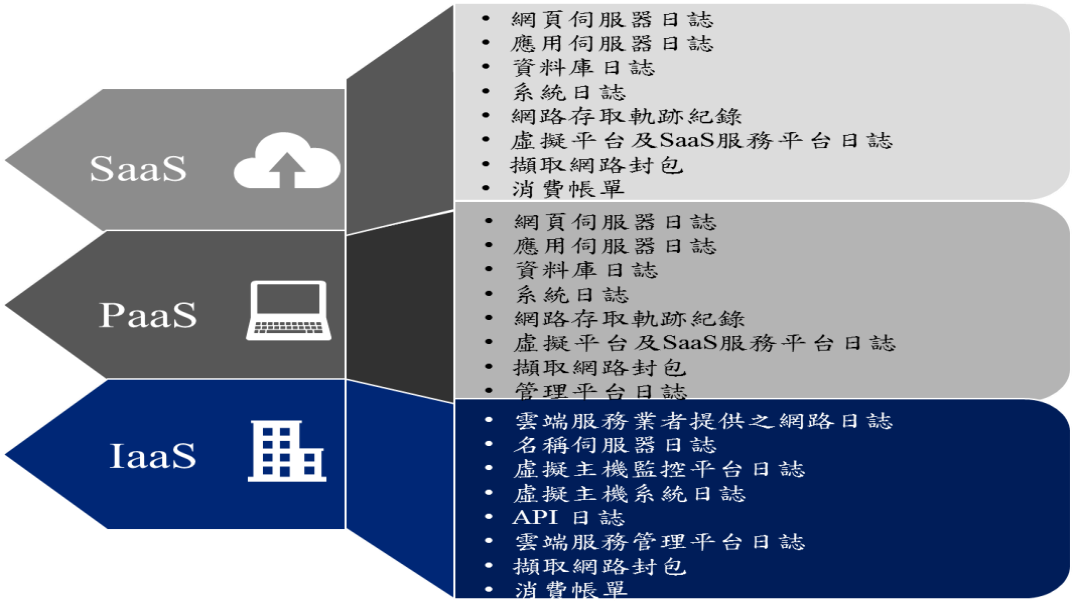
表二： 國外學者提出之數位鑑識建議作業程序

提出學者	建議作業程序
M. José [12]	1. 識別(Identification) 2. 保存(Preservation) 3. 蒐集(Collection） 4. 檢查分析(Analysis) 5. 呈現(Presented)
Eoghan Casey[4]	1. 數位證據辨識(Recognition） 2. 保存(Preservation） 3. 蒐集(Collection） 4. 分類(Classification） 5. 比對(Comparison） 6. 個化(Individualization） 7. 重建(Reconstruction)
Kuchta[8]	1. 準備工作(Preparation） 2. 紀錄與文件化(Documentation) 3. 收集(Collection) 4. 驗證(Authentication) 5. 分析(Analysis) 6. 保護(Preservation) 7. 產出結果(Production) 8. 報告文件(Reporting)
Deniz Sinangin[3]	1. 識別證據(Recognized) 2. 取得證據(Recovered) 3. 保護證據(Preserved) 4. 分析證據(Analyzed) 5. 展示證據(Presented)

三、各類雲端服務模式可擷取之資料內容

學者 Dobrosavljević[17]指出雲端與傳統數位鑑識差異最大部份為識別數位證據所在，因雲端資料可能為分散於多個實體儲存媒體，使用者甚至服務提供商都無法確認資料確切位置。關於雲端服務模式下可蒐集之數位證據項目，雲端安全聯盟於「Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing」[1]提及於 SaaS、PaaS 及 IaaS 環境

下可能存在之蒐集標的，整理如下圖四。



圖四： 雲端安全聯盟提出之雲端數位證據蒐集標的

Oliveira [12]亦以 ISO27037:2012[9]等國際規範為雲端鑑識架構基礎，提出各階段雲端鑑識將遇到之難題，文獻中提出可能存在於使用者本機端之雲端鑑識分析標的為「執行程序」、「記憶體」、「邏輯檔案」、「電子郵件」、「日誌軌跡」、「網路封包」及「網頁資料」等 7 項。

針對特定雲端服務探討數位證據留存項目部份，國外學者 Kadari[15]提出透過日誌模組(Log Module)擷取並分析 SaaS 與 PaaS 雲端服務日誌，鑑識人員可藉此架構，完整取得雲端日誌並有助於提昇數位證據之證據能力。另一方面，StaaS 雲端服務之數位證據留存部份，國內學者鍾敏如[20]等學者亦針對 Dropbox、Google Drive 及 OneDrive 等常見之 StaaS 服務產品透過建構模擬環境並實際測試上述雲端服務於使用者本機端所留下之數位證據及位置，整理如下表三

表三： 鍾敏如等學者提出之 StaaS 雲端服務證據標的

雲端服務	主機端軟體留存資料	瀏覽器留存資料	記憶體留存資料
Onedrive	同步資料夾、Log、OwnerID、Prefetch	使用者名稱、登入 Email	使用者名稱、密碼、檔案紀錄等
Dropbox	同步資料夾、Prefetch、加密檔案		使用者名稱、電腦名稱
Google Drive	同步資料夾、Prefetch	檔案資訊、登入 Email	使用者名稱、檔案紀錄

國外學者 Dykstra 等人[6]針對 IaaS 架構之特性、產品種類及留存證據等，分別探討各層可使用之擷取方式及標的，整理如下表四。並於隔年提出針對 OpenStack 私有雲架構之鑑識工具 FROST(Forensic OpenStack Tools)[7]，該工具可安裝於 OpenStack 之儀表板管理介面(Dashboard)、應用程序及網路套件中，並藉此蒐集特定雲端數位證據。

表四： Dykstra 等學者提出之 IaaS 雲端服務證據擷取方式等相關資訊

雲端架構層級	擷取方式	需取得之授權
網路層	封包側錄	網路設備
實體設備	存取實體硬碟	實體及網路設備
實體之作業系統	存取邏輯磁區	作業系統、實體及網路設備
虛擬化技術	虛擬內視技術	虛擬管理平台、作業系統、實體及網路設備
虛擬主機作業系統	遠端鑑識軟體	虛擬主機作業系統及上述各項軟硬體
軟體程式	因程式內之資料而異	軟體程式與上述各項軟硬體

四、雲端鑑識之挑戰

多數國內外雲端鑑識文獻皆有探討各種雲端服務環境下之挑戰，學者 Zawoad[16]整理常見雲端鑑識挑戰，並說明何種服務存在何種挑戰，整理如下表五。

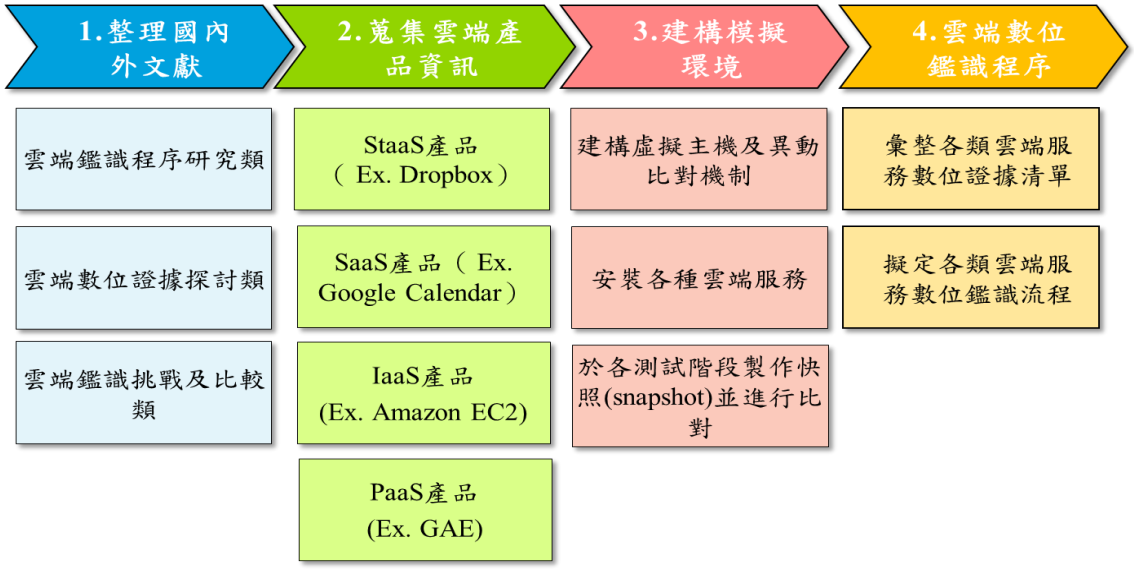
表五： Zawoad 等學者[16]提出之雲端數位鑑識挑戰

雲端鑑識挑戰	該挑戰存在於		
	IaaS	**PaaS**	**SaaS**
無法實體接觸	Y	Y	Y
需雲端服務商配合	Y	Y	Y
需依靠雲端服務商提供日誌	Y	Y	Y
分散磁碟儲存日誌檔案	Y	Y	Y
日誌分層存放	Y	Y	Y
需評估存取日誌可行性	Y	Y	Y
可能遺失關鍵日誌檔案	Y	Y	Y
部份日誌為揮發性資料	Y		
會有數位證據證明力問題	Y	Y	Y
會有證據監管鏈問題	Y	Y	Y
會有保存(Preservation)數位證據問題	Y	Y	Y
跨境執行鑑識時，會有法律問題	Y	Y	Y
現行鑑識工具無法支援	Y	Y	Y
需取得揮發性資料	Y		
擷取雲端數位證據需要較大網路頻寬	Y		
該雲端服務有多租戶情況	Y	Y	
無法重建犯罪現場	Y	Y	
會有合約問題	Y	Y	

參、研究方法

本研究發現多數既有文獻探討 ISO27037:2012[9]與雲端鑑識之差異，或列舉多種雲端鑑識之挑戰，以及雲端服務能留存之數位證據種類，惟並未以實際測試方式建構所有雲端服務平台，故無法完整具體瞭解雲端服務於本機端留存之數位證據種類及相關路徑

本研究即以國內外文獻基礎，先蒐集彙整各類雲端服務常見產品相關資訊，透過建構模擬雲端服務平台並實際測試各種雲端服務後，比較各操作階段前後差異內容，列舉可能的數位證據項目，進而提出符合各類雲端服務之識別、擷取及蒐集等數位鑑識流程。



圖五： 雲端鑑識程序研究流程

肆、 雲端數位證據及建議鑑識程序

一、雲端服務辨識及蒐集標的

雲端服務辨識及蒐集標的於不考慮中間網路層之數據封包、路由紀錄等項目情況下，可分為使用者本機端資訊設備(以下簡稱本機端)以及雲端服務伺服器端資訊設備(以下簡稱伺服器端)兩種，並詳細說明如下。

(一) 本機端常見數位證據種類

1. 系統日誌檔：以 IaaS 服務為例，使用者透過遠端桌面連線使用 IaaS 雲端服務時，系統日誌將留存連線位置(IP)、連線時間等重要訊息。
2. 作業系統登錄檔：若雲端服務需於本機端安裝同步或管理程式，則作業系統登錄檔中將明確記錄該程式相關設定及連線紀錄等資訊
3. 應用程式日誌：使用者執行雲端服務本機端程式進行資料傳輸、檔案編輯或管理等相關動作時，會記錄於應用程式日誌中。
4. 網路瀏覽紀錄：若雲端服務可透過網頁瀏覽器直接操作，分析本機端之網頁瀏覽歷程、Cookie、快取(Cache)或其他瀏覽器暫存檔將可發現使用雲端服務之稽證。
5. 應用程式安裝清單：此為較易檢視之識別雲端服務標的，鑑識人員可透過程式安裝清單快速釐清本機端是否有安裝雲端服務之本機端程式。
6. 應用程式同步資料夾：多數 StaaS 雲端服務會設定本機端與雲端同步之資料夾，預設為使用者帳號之資料夾路徑下，可作為識別是否有使用雲端服務之檢視項目
7. 程式 Prefetch 檔：執行程式後作業系統會留下暫存檔，副檔名為 PF，鑑識人員可藉此判斷該程式曾被執行過。

(二) 伺服器端常見數位證據種類

1. 儲存於雲端之資料：使用者存於 SaaS、StaaS 及 PaaS 雲端服務伺服器中之資料皆為擷取之重要標的，常以下載或備份方式取得雲端資料。若為 IaaS 雲端虛擬主機服務，其擷取資料之方式等同於執行一般作業系統數位鑑識，應考量作業系統特性，選擇適當之擷取方式。
2. 使用雲端服務之帳號相關資訊：伺服器端會記錄資料擁有者帳號、分享帳號、管理帳號及與帳號相關之設定值及建立時間等訊息。
3. 雲端服務之設定值及日誌：雲端服務管理介面會記錄可存取來源 IP、連線歷程、存取規則設定及其他與雲端服務平台相關之日誌

(三) 本機端與伺服器端皆有可能存放之數位證據

1. 記憶體資料：記憶體資料若能於案件發生後隨即保存，應可發現大量雲端服務操作資料或帳號密碼資訊
2. 特定副檔名之備份檔案：以 SaaS 之 Gmail 網頁郵件為例，使用者若透過備份工具進行信件備份，則會產生副檔名為「eml」之檔案，鑑識人員於識別

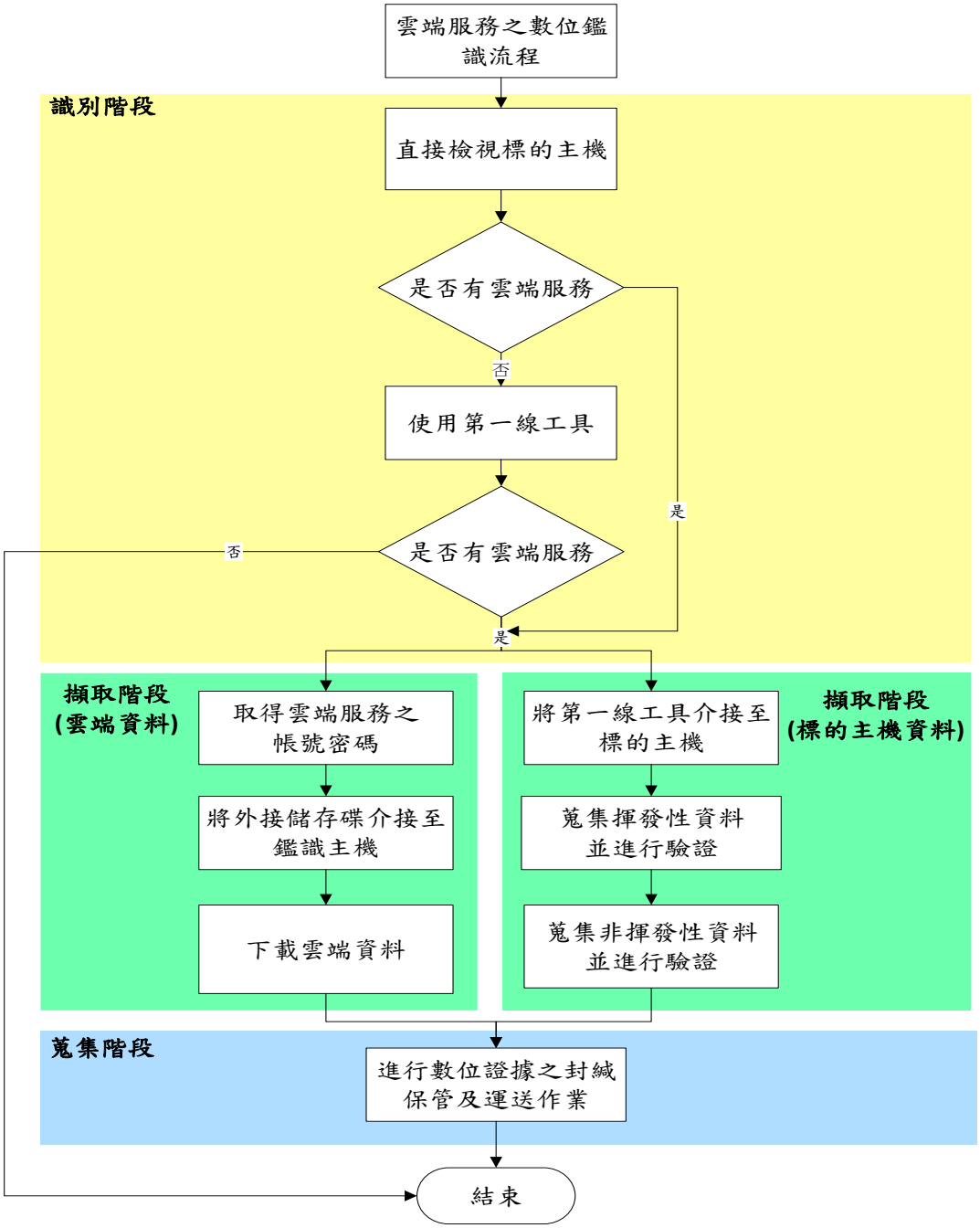
出本機端有使用雲端服務後，再深入瞭解該雲端服務是否有特定副檔名之檔案。

二、雲端鑑識建議程序

本研究根據實際於雲端數位鑑識模擬環境之測試結果，並參考 ISO27037:2012[8]之標準程序，提出分為識別、擷取及蒐集三個階段之雲端鑑識建議程序，部份步驟因考量數位證據之完整性、一致性及鑑識人員操作便利性，故建議使用適合之第一線數位鑑識工具進行該步驟。擷取階段因雲端服務特性，將分別針對本機端及伺服器端資料進行擷取。以下分別說明雲端鑑識整體建議程序及各類雲端服務鑑識程序要點，前者為歸納各雲端服務鑑識程序之共通點，說明各階段程序重點，後者分別敘述各類雲端服務之鑑識流程特點，使鑑識人員較能清楚雲端鑑識流程架構。

(四) 雲端鑑識建議程序

1. 識別階段：識別階段以確認標的主機是否有使用雲端資料為主，鑑識人員應避免過多擷取。本階段分為直接檢視標的主機及使用第一線數位鑑識工具兩種識別途徑，如前章節所述，部份雲端數位證據較容易直接檢視，用以識別使用何種雲端服務。若必須檢視較大量之資料(如網頁瀏覽記錄、系統日誌或記憶體資料等)，則鑑識人員應透過適合之第一線數位鑑識工具進行搜尋，避免過多人為操作。另外，本階段所識別之數位證據亦須透過適當方式進行數位證據擷取及封存程序
2. 擷取階段：進行擷取階段前，鑑識人員應先取得雲端服務之帳號密碼，並使用鑑識主機及外接硬碟進行雲端資料下載。本機端資料可依照既有之數位證據擷取流程，擷取揮發性及非揮發性資料。
3. 蒐集階段：由於雲端資料需以檔案形式進行擷取，故本階段將以存放雲端資料之外接硬碟作為原始證物，並進行後續封緘、保管及運作作業

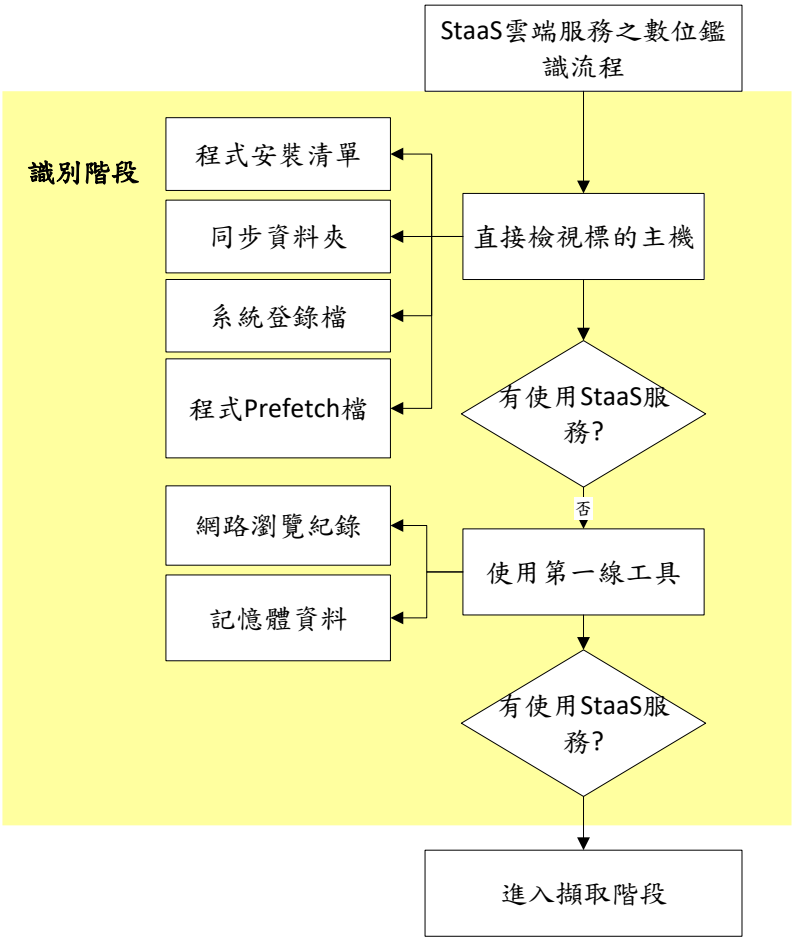


圖六： 雲端鑑識建議程序

(五) 各類雲端服務鑑識程序要點

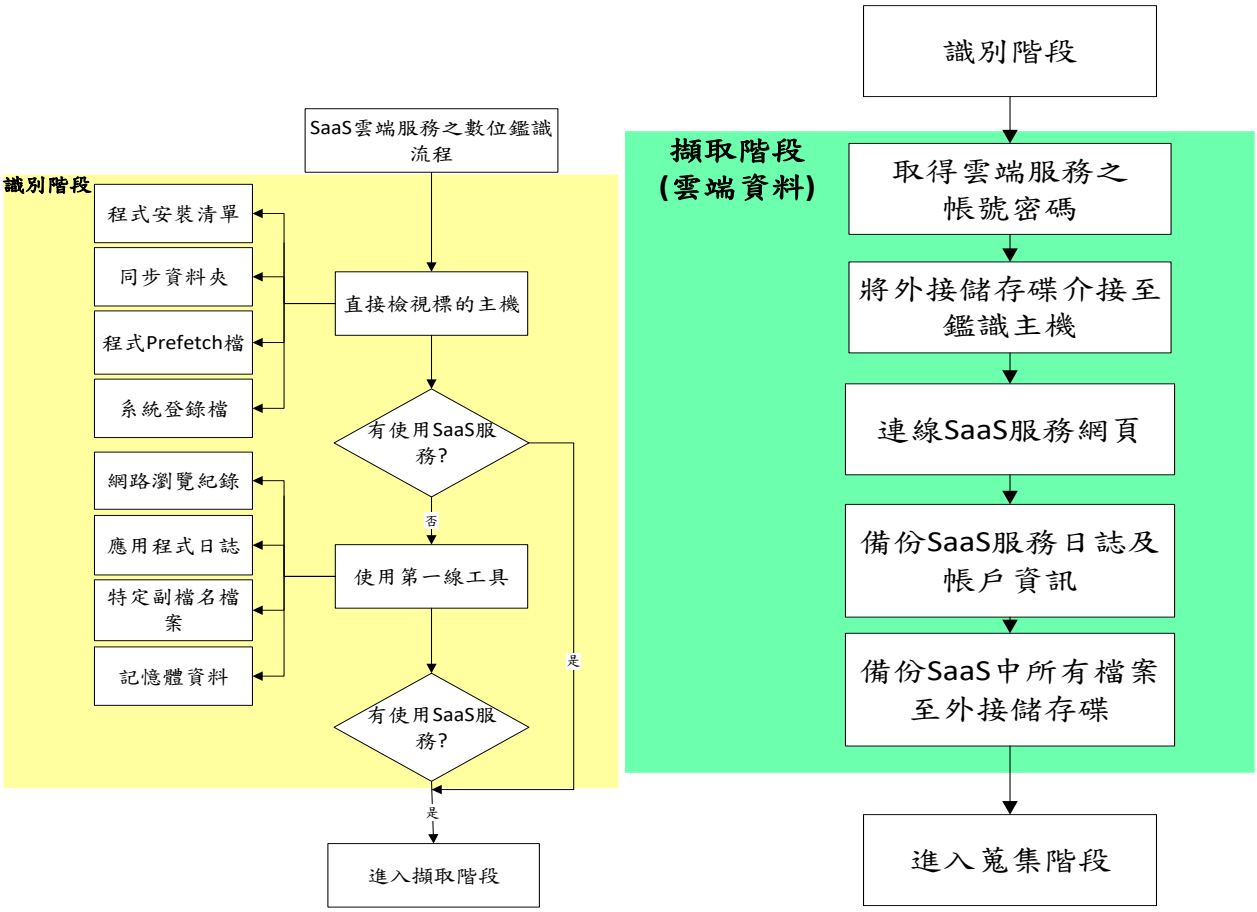
1. StaaS：使用 StaaS 雲端服務之途徑可分為以安裝程式或網頁瀏覽兩種方式，可透過應用程式清單及同步資料夾等直接檢視方式確認是否有使用該

服務。若無法直接檢視完成識別，則需以第一線數位鑑識工具蒐集網頁瀏覽紀錄後，並以特定關鍵字進行搜尋。



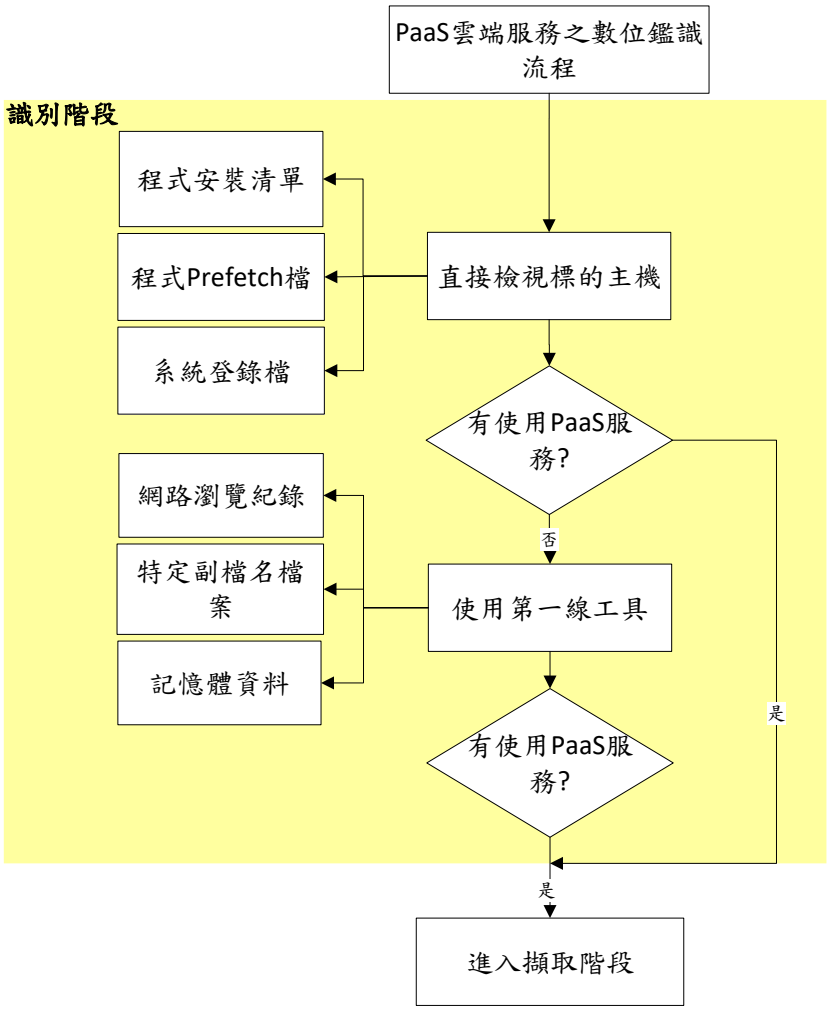
圖七： StaaS 識別階段要點

2. SaaS：常見之 SaaS 為電子郵件或共同編輯平台等服務，鑑識人員除針對安裝程式等資訊外，亦可以搜尋是否有特定副檔名之備份檔(例如 Google Calendar 之 ics 檔案)，進行識別。擷取階段時，除雲端服務中所有資料外，亦須針對服務管理平台之日誌及帳號等資訊進行擷取。且於本機端應依循既有之數位鑑識流程，針對揮發及非揮發性資料進行擷取作業。



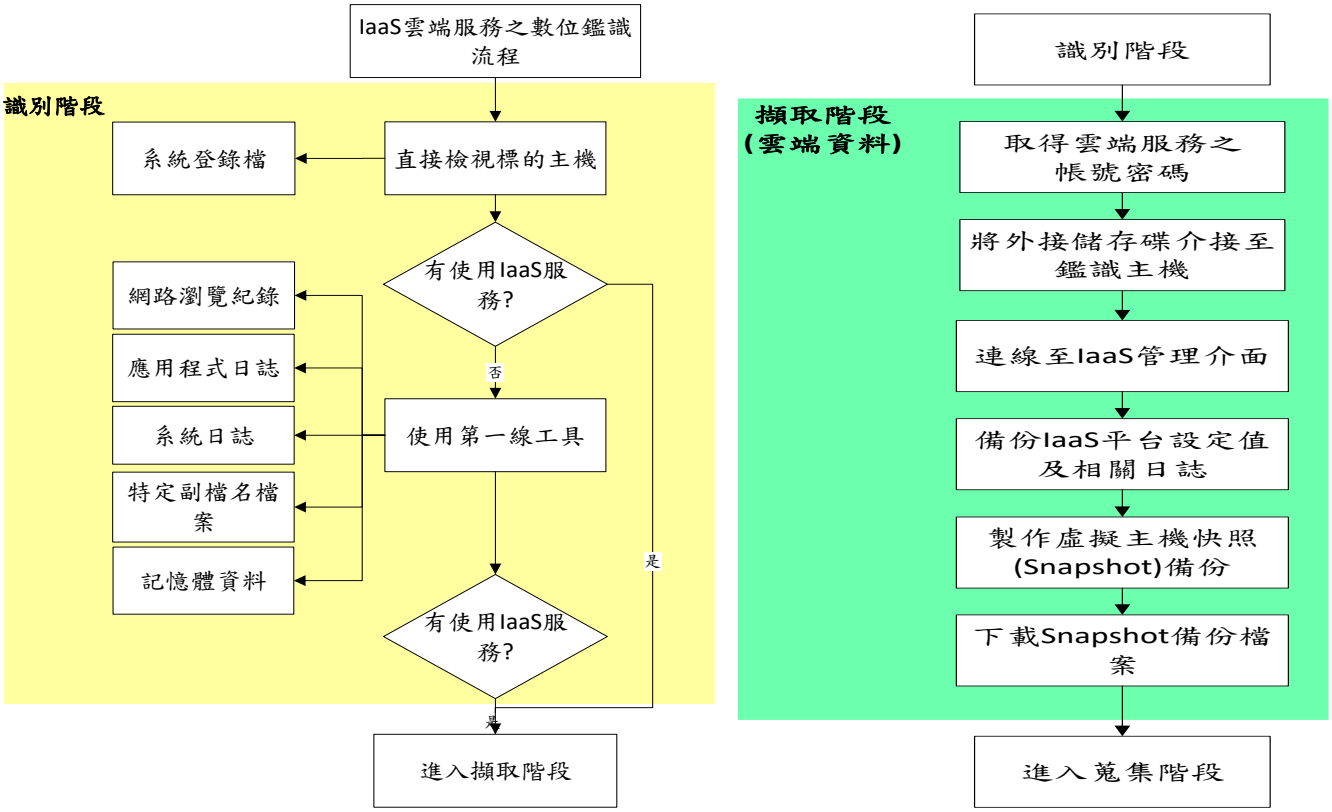
圖八： SaaS 識別及擷取階段要點

3. PaaS：若使用 PaaS 服務所開發之程式並未下載於本機端，則需針對本機端存取雲端服務之軌跡進行辨識及擷取，如於程式安裝清單中可檢視是否安裝 PaaS 雲端服務管理程式，於網頁瀏覽紀錄可搜尋特定網域名稱(如 GAE)。



圖九： PaaS 識別階段要點

4. IaaS：使用者常以遠端桌面連線或 VPN 連線至 IaaS 虛擬主機，故鑑識人員較無法透過直接檢視辨識本機端是否有使用 Iaas 服務，必須透過第一線數位鑑識工具擷取並搜尋關鍵字(如特定連線服務名稱)。擷取階段時，虛擬主機之快照(Snapshot)檔案及記憶體資料為本階段最主要之擷取標的。鑑識人員亦應擷取虛擬主機之管理介面會存放之使用者帳號、存取紀錄及相關設定值資訊。



圖十： IaaS 識別及擷取階段要點

伍、 結論與建議

一、結論

在雲端服務種類及雲端儲存資料皆已爆炸性成長的現在，許多企業仰賴雲端服務以節省營運成本，惟雲端鑑識技術對各國研究者都是仍在發展中的議題，且因雲端服務類別的種類繁多，既有的現場數位證據蒐證程序無法適用於不同類別之雲端鑑識作業，故應根據雲端服務之種類的不同加以分別訂定標準作業流程。

鑑識人員在面臨各類型雲端環境時，若能依循本研究之建議程序進行蒐證，除了能加速雲端蒐證作業之效率，亦能提昇鑑識人員之技術能力，並減少識別或蒐集雲端數位證據不完整之情況。

二、建議

本研究探討國內外相關文獻並實際建置模擬平台後發現，現行雲端資料擷取方式多由數位鑑識軟體與雲端服務直接取得，國外學者 Zhenbang[13]則提出擷取雲端資料之雲端數位鑑識中心架構，其可避免中斷雲端服務主機，並可改善擷取作業效率、驗證擷取作業、管理保護數位證據等多項議題，未來建議可朝此方向深入探討。

[誌謝]
本研究承蒙 103 年行政院國家科學技術發展技術管理會補助計畫(計畫編號 MOST 103-3114-Y-138-003)之經費補助，謹此致謝。

參考文獻

[1] Cloud Security Alliance, “Incident Management and Forensics Working Group:Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing”, pp.6-8, 2013.
[2] Cloud Security Alliance, “Incident Management and Forensics Working Group:Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing”, pp.13-26, 2013.
[3] S. Deniz, “Computer Forensics Investigations in a Corporate Environment”, IEEE computer fraud & Security, pp.272, 2002.
[4] C. Eoghan, “Digital Evidence and Computer Crime”, pp187-197,2011.
[5] L. Fang, T. Jin, M. Jian, B. Robert, M. John, B. Lee and L. Dawn, ”NIST Cloud Computing Reference Architecture(SP500-292), National Institute of Standards and Technology” , pp.3, 2011.
[6] D. Josiah and S. Alan, “Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing:Exploring and Evaluating Tools, Trust, and Techniques”, 2012.
[7] D. Josiah and S. Alan, “Design and implementation of FROST Digital forensic tools”, Digital Investigation ,vol. 10, pp.87-95, 2013.
[8] K. J. Kuchta and J. Kelly, “Forensic Fieldwork: Experience Is the Best Teacher”, Information Systems Security, vol. 3, Issue:1, pp.29-33,2002.
[9] International Standard Organization, ”ISO/IEC 27037”, 2012.
[10] International Standard Organization, ”ISO/IEC 27041”, 2015.
[11] International Standard Organization, ”ISO/IEC 27042”, 2015.
[12] M. José, and C. Marcelo, “Best Practice and challenges for process efficiency of investigations and digital forensics.”, DOI: 10.5769/C2013003, 2013.

[13] Z. Liu and H. Zou, “POSTER: A Proactive Cloud-Based Cross-Reference Forensic Framework”, 21st ACM Conference on Computer and Communications Security, pp.1475-1477, 2014.

[14] M. Peter and G. Timothy, ” The NIST Definition of Cloud Computing (SP800-145), National Institute of Standards and Technology”, pp.2-3, 2011.

[15] K. Raju and K. Janapati, “Securing Digital Forensics on Cloud Computing through Log based Accession”, 2014.

[16] Z. Shams and H. Ragib, “Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems”, arXiv:1302.6312v1 [cs.DC], 2013.

[17] D. Vladimir, V. Mladen and B. Ivan, “STANDARD IMPLEMENTATION IN CLOUD FORENSICS”, 2015.

[18] L. Yunting and C. Yuyin,”Research on Live Forensics in Cloud Environment”, 2nd International Symposium on Computer, Communication, Control and Automation., 2013.

[19] 周瑞國、林宜隆、伍台國， “植基於雲端安全之數位證據鑑識標準作業程序之研究” ，2011。

[20] 鐘敏如、王旭正，”Evidence Investigations in Forensics in Case of Clouding Access with Data Synchronizations” ，TANET2013 臺灣網際網路研討會，2013。